

#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTY. DOCKET NO. 040373-0263

In re Patent Application of

Koji MANABE

Serial No. Unassigned

Filed: September 24, 1999

For: WORKS PROTECTING SYSTEM AND WORKS PROTECTING  
METHOD THEREFOR

10678 U.S. PTO  
09/404712  
09/24/99

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. 119, is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application  
No. 10-278153 filed September 30, 1998.

Respectfully submitted,

September 24, 1999  
Date

*David A. Blumenthal* 36489  
David A. Blumenthal  
Reg. No. 26,257

FOLEY & LARDNER  
3000 K Street, N.W., Suite 500  
Washington, D.C. 20007-5109  
Tel: (202) 672-5300

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

manabe  
040373/0263

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

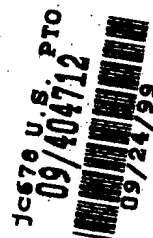
1998年 9月30日

出願番号  
Application Number:

平成10年特許願第278153号

出願人  
Applicant(s):

日本電気株式会社

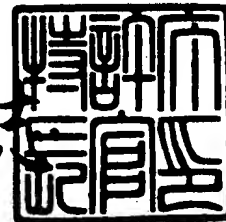


CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年 4月 2日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3019978

【書類名】 特許願

【整理番号】 68501622

【提出日】 平成10年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/06  
G06F 12/14

【発明の名称】 著作物保護システムおよびその著作物保護方法

【請求項の数】 6

【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

【氏名】 真鍋 浩嗣

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100070219

【弁理士】

【氏名又は名称】 若林 忠

【電話番号】 03-3585-1882

【選任した代理人】

【識別番号】 100100893

【弁理士】

【氏名又は名称】 渡辺 勝

【選任した代理人】

【識別番号】 100088328

【弁理士】

【氏名又は名称】 金田 暢之

【選任した代理人】

【識別番号】 100106138

【弁理士】

【氏名又は名称】 石橋 政幸

【選任した代理人】

【識別番号】 100106297

【弁理士】

【氏名又は名称】 伊藤 克博

【手数料の表示】

【予納台帳番号】 015129

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9710078

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 著作物保護システムおよびその著作物保護方法

【特許請求の範囲】

【請求項 1】 著作物を伝送する A V データ送信機器と、該著作物を受信する相手側の送受信機器とから構成され、

前記 A V データ送信機器は、コマンド入力手段と、コマンド制御手段と、A V データ送信手段と、暗号化手段と、第 1 の認証手段と、第 1 の入出力手段と、機器 I D 検出手段と、認証履歴記憶手段とを備えて構成され、

前記相手側の送受信機器は、第 2 の入出力手段と、A V データ受信手段と、復号化手段と、第 2 の認証手段とを備えて構成され、

前記認証手段は、過去に認証を行った履歴がある前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項 2】 著作物を伝送する A V データ送信機器と、該著作物を受信する複数の相手側の送受信機器とから構成され、

前記 A V データ送信機器は、コマンド入力手段と、コマンド制御手段と、A V データ送信手段と、暗号化手段と、第 1 の認証手段と、第 1 の入出力手段と、機器 I D 検出手段と、認証履歴記憶手段と、暗号鍵記憶手段とを備えて構成され、

前記複数の相手側の送受信機器は、それぞれ第 2 の入出力手段と、A V データ受信手段と、復号化手段と、第 2 の認証手段とを備えて構成され、

前記認証手段は、過去に認証を行った履歴がある前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項 3】 著作物を伝送する A V データ送信機器と、該著作物を受信する相手側の送受信機器とから構成され、

前記 A V データ送信機器は、コマンド入力手段と、コマンド制御手段と、A V データ送信手段と、暗号化手段と、第 1 の認証手段と、第 1 の入出力手段と、機

器 I D 検出手段とを備えて構成され、

前記相手側の送受信機器は、第 2 の入出力手段と、A V データ受信手段と、復号化手段と、第 2 の認証手段とを備えて構成され、

前記認証手段は、前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項 4】 前記機器 I D 検出手段により、前記相手側の送受信機器 I D を検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記相手側の送受信機器 I D が含まれているかどうかを調べる段階と、

前記履歴情報の中に前記相手側の送受信機器 I D が含まれている場合、前記第 1 の認証手段により、相手側の前記第 2 の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

その後、前記コマンド入力手段に対してユーザから A V データ送信指示のコマンド入力があると、前記コマンド制御手段を介して前記 A V データ送信手段に前記コマンドが通知され、前記 A V データ送信手段により、前記 A V データの送信を開始する段階と、

前記履歴情報の中に前記相手側の送受信機器 I D が含まれていない場合、前記コマンド入力手段に対してユーザから A V データ送信指示のコマンド入力があるのを待つ段階と、

該 A V データ送信指示のコマンド入力があると、前記第 1 の認証手段により、相手側の前記第 2 の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記相手側の送受信機器 I D を履歴情報として記録する段階と、

前記コマンド制御手段を介して前記 A V データ送信手段に前記コマンドが通知され、前記 A V データ送信手段により、前記 A V データの送信を開始する段階と

前記暗号化手段により、前記A Vデータを前記暗号鍵を用いて暗号化し、前記第1の入出力手段へ送出する段階と、

該第1の入出力手段により、前記暗号化されたA Vデータを伝送路に送出する段階と、

前記第2の入出力手段により、前記暗号化されたA Vデータを前記伝送路から受け取る段階と、

前記復号化手段により、前記暗号化されたA Vデータを前記暗号鍵を用いて復号化し、前記A Vデータ受信手段へ送出する段階と、

該A Vデータ受信手段により、前記復号化されたA Vデータを受け取る段階とを有する請求項1に記載の著作物保護システムの著作物保護方法。

【請求項5】 前記機器ID検出手段により、第1の相手側の送受信機器IDを検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記第1の相手側の送受信機器IDが含まれているかどうかを調べる段階と、

前記履歴情報の中に前記第1の相手側の送受信機器IDが含まれている場合、前記第1の認証手段により、第1の相手側の前記第2の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記鍵交換作業の結果、共有した暗号鍵を第1の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記機器ID検出手段により、第2の相手側の送受信機器IDを検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記第2の相手側の送受信機器IDが含まれているかどうかを調べる段階と、

前記履歴情報の中に前記第2の相手側の送受信機器IDが含まれている場合、前記第1の認証手段により、第2の相手側の前記第2の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記鍵交換作業の結果、共有した暗号鍵を第2の暗号鍵として暗号鍵記憶手段に記録する段階と、

その後、前記コマンド入力手段に対してユーザから前記第1の相手側の送受信

機器または前記第2の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があると、前記コマンド制御手段を介して前記AVデータ送信手段に前記コマンドが通知され、前記AVデータ送信手段により、前記AVデータの送信を開始する段階と、

前記履歴情報の中に前記第1の相手側の送受信機器IDが含まれていない場合

、

前記コマンド入力手段に対してユーザから前記第1の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があるのを待つ段階と、

該AVデータ送信指示のコマンド入力があると、前記第1の認証手段により、前記第1の相手側の前記第2の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記第1の相手側の送受信機器IDを履歴情報として記録する段階と、

前記鍵交換作業の結果、共有した暗号鍵を第1の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記履歴情報の中に前記第2の相手側の送受信機器IDが含まれていない場合

、

前記コマンド入力手段に対してユーザから前記第2の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があるのを待つ段階と、

該AVデータ送信指示のコマンド入力があると、前記第1の認証手段により、前記第2の相手側の前記第2の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記第2の相手側の送受信機器IDを履歴情報として記録する段階と、

前記鍵交換作業の結果、共有した暗号鍵を第2の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記コマンド制御手段を介して前記AVデータ送信手段に前記コマンドが通知され、前記AVデータ送信手段により、前記第1の相手側の送受信機器または前記第2の相手側の送受信機器に対してのAVデータの送信を開始する段階と、



前記コマンド入力手段に対してユーザから前記第 1 の相手側の送受信機器に対しての A V データ送信指示のコマンド入力がある場合は、

前記暗号化手段により、前記 A V データを前記第 1 の暗号鍵を用いて暗号化し、前記第 1 の入出力手段へ送出する段階と、

該第 1 の入出力手段により、前記暗号化された A V データを伝送路に送出する段階と、

前記第 1 の相手側の第 2 の入出力手段により、前記暗号化された A V データを前記伝送路から受け取る段階と、

前記第 1 の相手側の復号化手段により、前記暗号化された A V データを前記第 1 の暗号鍵を用いて復号化し、前記第 1 の相手側の A V データ受信手段へ送出する段階と、

該 A V データ受信手段により、前記復号化された A V データを受け取る段階と、

前記コマンド入力手段に対してユーザから前記第 2 の相手側の送受信機器に対しての A V データ送信指示のコマンド入力がある場合は、

前記暗号化手段により、前記 A V データを前記第 2 の暗号鍵を用いて暗号化し、前記第 1 の入出力手段へ送出する段階と、

該第 1 の入出力手段により、前記暗号化された A V データを伝送路に送出する段階と、

前記第 2 の相手側の第 2 の入出力手段により、前記暗号化された A V データを前記伝送路から受け取る段階と、

前記第 2 の相手側の復号化手段により、前記暗号化された A V データを前記第 2 の暗号鍵を用いて復号化し、前記第 2 の相手側の A V データ受信手段へ送出する段階と、

該 A V データ受信手段により、前記復号化された A V データを受け取る段階とを有する請求項 2 に記載の著作物保護システムの著作物保護方法。

【請求項 6】 前記 A V データの伝送路は I E E E 1 3 9 4 高速シリアルバスである請求項 4 または請求項 5 に記載の著作物保護システムの著作物保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、AVデータを送受信する際の機器間の著作物保護システム及びその著作物保護方法に関する。

【0002】

【従来の技術】

従来、ユーザにアナログデータとして扱われてきたAVデータが、近年、デジタル衛星放送、インターネット配信、DVDなどの普及によってデジタルデータのまま扱われるようになった。またデジタルデータを高速に伝送できるIEEE1394高速シリアルバスが実用化されるに至り、著作権保護の観点からAVデータを送受信する際の機器間の著作物保護システムが提案されている。

【0003】

例えば、日経エレクトロニクス1998.3.23pp.47-53「IEEE1394のコピー防止技術、公開鍵/共通鍵併用で一本化」には認証手段および暗号化手段を備える著作物保護システムが示されている。そのシステムのブロック図を図4に示し、状態遷移図を図5に示す。この従来の著作物保護システムの構成は次の通りである。コマンド入力手段11に対してユーザからAVデータ送信指示があると(S11)、コマンド制御手段21を介して認証手段51は相手側の認証手段141と認証を行う(S12)。認証を終えると、AVデータ送信手段31はAVデータの送信を開始する(S13)。AVデータは暗号化手段41において暗号鍵を用いて暗号化され入出力手段61を介して伝送路に送出される。相手側の送受信機器において、入出力手段111は伝送路から暗号化されたAVデータを受け取る。復号化手段131は暗号化されたAVデータを暗号鍵を用いて復号し、AVデータ受信手段121は復号化されたAVデータを受け取る。

【0004】

【発明が解決しようとする課題】

上述の説明で明らかなように、従来の著作物保護システムはユーザからAVデ

ータ伝送指示があつてはじめて相手側の送受信機器と認証を行うため、A Vデータを伝送するまでに時間がかかるという問題があつた。

【0005】

上述の従来技術の問題点に鑑み、本発明の目的は、A Vデータ伝送指示からA Vデータを伝送するまでの時間を短縮する著作物保護システム及びその著作物保護方法を提供することにある。

【0006】

【課題を解決するための手段】

本発明の著作物保護システムは、

著作物を伝送するA Vデータ送信機器と、著作物を受信する相手側の送受信機器とから構成され、A Vデータ送信機器は、コマンド入力手段と、コマンド制御手段と、A Vデータ送信手段と、暗号化手段と、第1の認証手段と、第1の入出力手段と、機器ID検出手段と、認証履歴記憶手段とを備えて構成され、相手側の送受信機器は、第2の入出力手段と、A Vデータ受信手段と、復号化手段と、第2の認証手段とを備えて構成され、認証手段は、過去に認証を行った履歴がある相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である。

【0007】

また、著作物を伝送するA Vデータ送信機器と、著作物を受信する複数の相手側の送受信機器とから構成され、A Vデータ送信機器は、コマンド入力手段と、コマンド制御手段と、A Vデータ送信手段と、暗号化手段と、第1の認証手段と、第1の入出力手段と、機器ID検出手段と、認証履歴記憶手段と、暗号鍵記憶手段とを備えて構成され、複数の相手側の送受信機器は、それぞれ第2の入出力手段と、A Vデータ受信手段と、復号化手段と、第2の認証手段とを備えて構成され、認証手段は、過去に認証を行った履歴がある相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段であつてもよい。

## 【0008】

また、著作物を伝送するAVデータ送信機器と、著作物を受信する相手側の送受信機器とから構成され、AVデータ送信機器は、コマンド入力手段と、コマンド制御手段と、AVデータ送信手段と、暗号化手段と、第1の認証手段と、第1の入出力手段と、機器ID検出手段とを備えて構成され、相手側の送受信機器は、第2の入出力手段と、AVデータ受信手段と、復号化手段と、第2の認証手段とを備えて構成され、認証手段は、相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段であってもよい。

## 【0009】

本発明の著作物保護システムの著作物保護方法は、

機器ID検出手段により、相手側の送受信機器IDを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に相手側の送受信機器IDが含まれているかどうかを調べる段階と、履歴情報の中に相手側の送受信機器IDが含まれている場合、第1の認証手段により、相手側の第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、その後、コマンド入力手段に対してユーザからAVデータ送信指示のコマンド入力があると、コマンド制御手段を介してAVデータ送信手段にコマンドが通知され、AVデータ送信手段により、AVデータの送信を開始する段階と、履歴情報の中に相手側の送受信機器IDが含まれていない場合、コマンド入力手段に対してユーザからAVデータ送信指示のコマンド入力があるのを待つ段階と、AVデータ送信指示のコマンド入力があると、第1の認証手段により、相手側の第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に相手側の送受信機器IDを履歴情報として記録する段階と、コマンド制御手段を介してAVデータ送信手段にコマンドが通知され、AVデータ送信手段により、AVデータの送信を開始する段階と、暗号化手段により、AVデータを暗号鍵を用いて暗号化し、第1の入出力手段へ送出する段階と、第1の入出力手段により、暗号化されたAVデータを伝送路に送出する段階と、第2の入出力手段により、暗号化された

AVデータを伝送路から受け取る段階と、復号化手段により、暗号化されたAVデータを暗号鍵を用いて復号化し、AVデータ受信手段へ送出する段階と、AVデータ受信手段により、復号化されたAVデータを受け取る段階とを有する。

【0010】

また、機器ID検出手段により、第1の相手側の送受信機器IDを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に第1の相手側の送受信機器IDが含まれているかどうかを調べる段階と、履歴情報の中に第1の相手側の送受信機器IDが含まれている場合、第1の認証手段により、第1の相手側の第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、鍵交換作業の結果、共有した暗号鍵を第1の暗号鍵として暗号鍵記憶手段に記録する段階と、機器ID検出手段により、第2の相手側の送受信機器IDを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に第2の相手側の送受信機器IDが含まれているかどうかを調べる段階と、履歴情報の中に第2の相手側の送受信機器IDが含まれている場合、前記第1の認証手段により、第2の相手側の前記第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、鍵交換作業の結果、共有した暗号鍵を第2の暗号鍵として暗号鍵記憶手段に記録する段階と、その後、コマンド入力手段に対してユーザから第1の相手側の送受信機器または第2の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があると、コマンド制御手段を介してAVデータ送信手段にコマンドが通知され、AVデータ送信手段により、AVデータの送信を開始する段階と、履歴情報の中に第1の相手側の送受信機器IDが含まれていない場合、コマンド入力手段に対してユーザから第1の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があるのを待つ段階と、AVデータ送信指示のコマンド入力があると、第1の認証手段により、第1の相手側の第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に第1の相手側の送受信機器IDを履歴情報として記録する段階と、鍵交換作業の結果、共有した暗号鍵を第1の暗号鍵として暗号鍵記憶手段に記録する段階と、履歴情報の中に第2の相手側の送受信機器IDが含まれていない場合、コマンド入力手段に対してユーザから第2の相手側の送受信機器に対してのAVデータ送信指示のコマ

ンド入力があるのを待つ段階と、A Vデータ送信指示のコマンド入力があると、第1の認証手段により、第2の相手側の第2の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に第2の相手側の送受信機器IDを履歴情報として記録する段階と、鍵交換作業の結果、共有した暗号鍵を第2の暗号鍵として暗号鍵記憶手段に記録する段階と、コマンド制御手段を介してA Vデータ送信手段にコマンドが通知され、A Vデータ送信手段により、第1の相手側の送受信機器または第2の相手側の送受信機器に対してのA Vデータの送信を開始する段階と、コマンド入力手段に対してユーザから第1の相手側の送受信機器に対してのA Vデータ送信指示のコマンド入力がある場合は、暗号化手段により、A Vデータを第1の暗号鍵を用いて暗号化し、第1の入出力手段へ送出する段階と、第1の入出力手段により、暗号化されたA Vデータを伝送路に送出する段階と、第1の相手側の第2の入出力手段により、暗号化されたA Vデータを伝送路から受け取る段階と、第1の相手側の復号化手段により、暗号化されたA Vデータを第1の暗号鍵を用いて復号化し、第1の相手側のA Vデータ受信手段へ送出する段階と、A Vデータ受信手段により、復号化されたA Vデータを受け取る段階と、コマンド入力手段に対してユーザから第2の相手側の送受信機器に対してのA Vデータ送信指示のコマンド入力がある場合は、暗号化手段により、A Vデータを第2の暗号鍵を用いて暗号化し、第1の入出力手段へ送出する段階と、第1の入出力手段により、暗号化されたA Vデータを伝送路に送出する段階と、第2の相手側の第2の入出力手段により、暗号化されたA Vデータを伝送路から受け取る段階と、第2の相手側の復号化手段により、暗号化されたA Vデータを第2の暗号鍵を用いて復号化し、第2の相手側のA Vデータ受信手段へ送出する段階と、A Vデータ受信手段により、復号化されたA Vデータを受け取る段階とを有してもよい。

【0011】

また、A Vデータの伝送路はIEEE 1394高速シリアルバスであってもよい。

【0012】

本発明の著作物保護システムおよびその著作物保護方法は、過去に認証を行っ

た履歴がある送受信機器が伝送路に接続すると、機器認証および鍵交換を行うことを特徴とするものであり、ユーザからのコマンド入力時点から著作物伝送開始までの時間を従来に比較して大幅に短縮するものである。

## 【0013】

機器ID検出手段は相手側の送受信機器が伝送路に接続すると、入出力手段を介して、その機器IDを検出する。ここで伝送路としては、例えば、IEEE1394高速シリアルバスを使うことが可能であり、また、相手側の送受信機器とは、例えば、入出力手段、AVデータ受信手段、復号化手段、認証手段を備えて構成される著作物の送受信機器である。機器ID検出手段が相手側の送受信機器の機器IDを検出すると、認証履歴記憶手段が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる。

## 【0014】

もし、履歴情報の中にその機器IDが含まれている場合、認証手段は相手側の認証手段と認証を行う。ここで認証とは、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業であり、また、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業である。その後いつでも、コマンド入力手段に対してユーザからAVデータ送信指示があると、コマンド制御手段を介してAVデータ送信手段にそのコマンドが通知され、AVデータ送信手段はAVデータの送信を開始する。AVデータは暗号化手段において暗号鍵を用いて暗号化され入出力手段を介してIEEE1394高速シリアルバスなどの伝送路に送出される。相手側の送受信機器において、入出力手段はIEEE1394高速シリアルバスなどの伝送路から暗号化されたAVデータを受け取る。復号化手段は暗号化されたAVデータを暗号鍵を用いて復号し、AVデータ受信手段は復号化されたAVデータを受け取る。

## 【0015】

もし履歴情報の中に機器IDが含まれていない場合、コマンド入力手段に対してユーザからAVデータ送信指示が来るのを待つ。AVデータ送信指示があると、認証手段は相手側の認証手段と認証を行う。認証を終えると、認証履歴記憶手段に相手側の機器IDを履歴情報として記録する。AVデータ送信手段はAVデ

ータの送信を開始する。A Vデータは暗号化手段において暗号鍵を用いて暗号化され入出力手段を介して伝送路に送出される。相手側の送受信機器において、入出力手段は伝送路から暗号化されたA Vデータを受け取る。復号化手段は暗号化されたA Vデータを暗号鍵を用いて復号し、A Vデータ受信手段は復号化されたA Vデータを受け取る。

【0016】

【発明の実施の形態】

(本発明の第1の実施の形態)

図1は本発明の第1の実施の形態の著作物保護システムの構成を示すブロック図である。図1を参照すると、機器ID検出手段70は相手側の送受信機器が伝送路に接続すると、入出力手段60を介して、その機器IDを検出する。ここで伝送路としては、例えば、IEEE1394高速シリアルバスが好適である。また、相手側の送受信機器とは、例えば、入出力手段110、A Vデータ受信手段120、復号化手段130、認証手段140を備えて構成される著作物の送受信機器であり、具体的には、デジタルテレビ受像機、書き込み可能なDVD装置すなわちDVD-RAM、デジタル方式のVTRすなわちD-VHSなどが好適である。機器ID検出手段70が相手側の送受信機器の機器IDを検出すると、認証履歴記憶手段80が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる。もし、履歴情報の中にその機器IDが含まれている場合、認証手段50は相手側の認証手段140と認証を行う。

【0017】

ここで認証とは、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とからなる。認証のためのデジタル署名方式および鍵配送方式はこれまで考案されている様々な方式を用いることが可能であるが、楕円DSA(Digital Signature Algorithm)署名および楕円DH(Diffie-Hellman)鍵配送を用いることが好適である。楕円DSA署名(以下EC-DSAという)について以下に述べる。EC-DSAはANSI X9.62などに規定されており、その内容は、鍵生成、署名生成、署名照合の三つの段階からなる。



【0018】

まず、鍵生成の手順は次の通りである。

【0019】

(1) EC-DSA鍵生成

デバイスAにおいて

1.  $ZP$ 上に構成する楕円曲線 $E$ を選択する。 $E(ZP)$ 上の点の数は大きな素数 $n$ で割り切れること。
2. 位数 $n$ の点 $P \in E(ZP)$ を選択する。
3. 区間  $[1, n-1]$ のなかから静的に特有かつ予言できない整数 $d$ を選択する。
4.  $Q = dP$ を計算する。
5. Aの公開鍵は $(E, P, n, Q)$ 、Aの秘密鍵は $d$ とする。

【0020】

つぎに、署名生成手順は以下の通りである。

【0021】

(2) EC-DSA署名生成

デバイスAにおいて、以下のようにメッセージ $m$ を暗号化する。

1. 区間  $[1, n-1]$ のなかから静的に特有かつ予言できない整数 $k$ を選択する。
2.  $kP = (x_1, y_1)$  および  $r = x_1 \bmod n$ を計算する。ここで $x_1$ はたとえばバイナリ表現からの変換によって一つの整数と見なされる。もし $r = 0$ ならばステップ1に戻る（セキュリティ上の理由である。 $r = 0$ なら暗号等式  $s = k^{-1} \{h(m) + dr\} \bmod n$  が秘密鍵 $d$ を含まないためである。）。
3.  $k^{-1} \bmod n$ を計算する。
4.  $s = k^{-1} \{h(m) + dr\} \bmod n$ を計算する。ここで $h$ はセキュアハッシュアルゴリズム（SHA-1）である。
5. もし $s = 0$ ならばステップ1に戻る（もし $s = 0$ ならば、 $s^{-1} \bmod n$ が存在しない。； $s^{-1}$ は署名照合のステップ2で必要である。）。

6. メッセージ $m$ の署名を整数の組み $(r, s)$ とする。

【0022】

さらに署名照合の手順は以下の通りである。

【0023】

(3) EC-DSA署名照合

$m$ のなかのデバイスAの署名 $(r, s)$ を照合するために、デバイスBは以下のことを行う。

1. Aの公開鍵 $(E, P, n, Q)$ の真のコピーを得る。
2.  $r$ および $s$ が区間 $[1, n-1]$ の整数であることを照合する。
3.  $w = s^{-1} \bmod n$ および $h(m)$ を計算する。
4.  $u_1 = h(m)w \bmod n$ および $u_2 = rw \bmod n$ を計算する。
5.  $u_1P + u_2Q = (x_0, y_0)$ および $v = x_0 \bmod n$ を計算する。
6.  $v = r$ ならば署名を認める。

【0024】

つぎに楕円DH鍵配送(以下EC-DHという)について述べる。EC-DHはANSI X9.63などに規定されており、その内容は鍵生成および交換と鍵共有の二つの段階からなる。

【0025】

まず、鍵生成および交換の手順は以下の通りである。

【0026】

(1) EC-DH鍵生成および交換

デバイスAにおいて

1. 区間 $[2, n-2]$ のなかから静的に特有かつ予言できない整数 $x$ を選択する。
2.  $a = xP$ を計算する。
3. デバイスAはデバイスBに $a$ を送る。

【0027】

デバイスBにおいて

1. 区間 $[2, n-2]$ のなかから静的に特有かつ予言できない整数 $y$ を選択す

る。

2.  $b = yP$  を計算する。

1. デバイス B はデバイス A に  $b$  を送る。

【0028】

次に鍵共有の手順を以下に述べる。

【0029】

(2) EC-DH 鍵共有

1. デバイス A において  $KA = x b = x y P$  により共通鍵を生成する。

2. デバイス B において  $KB = x a = x y P$  により共通鍵を生成する。

3.  $KA = KB$  なのでデバイス A とデバイス B は鍵を共有する。

【0030】

認証を終えると、その後いつでも、コマンド入力手段 10 に対してユーザから AV データ送信指示があると、コマンド制御手段 20 を介して AV データ送信手段 30 にそのコマンドが通知され、AV データ送信手段 30 は AV データの送信を開始する。コマンド入力手段としては、例えば、キーボードやマウス、リモコンなどが好適である。AV データとしては、様々なフォーマットの AV データを扱うことが可能であり、MPEG2 規格に準じて圧縮されたトランスポートストリームが好適である。AV データ送信手段 30 とは、例えばデジタル衛星放送受信装置、インターネットからの AV データ受信装置、DVD 装置などが好適である。AV データは暗号化手段 40 において暗号鍵を用いて暗号化され入出力手段 60 を介して IEEE 1394 高速シリアルバスなどの伝送路に送出される。

【0031】

暗号化手段で用いる暗号方式としては、これまでに考案されている様々なブロック暗号を用いることが可能である。例えば、ブローフィッシュ暗号が好適である。相手側の送受信機器において、入出力手段 110 は IEEE 1394 高速シリアルバスなどの伝送路から暗号化された AV データを受け取る。復号化手段 130 は暗号化された AV データを暗号鍵を用いて復号し、AV データ受信手段 120 は復号化された AV データを受け取る。ここで AV データは相手側の送受信機器が、デジタルテレビ受像装置であれば必要により MPEG2 デコード処理

を施された後表示、オーディオ出力され、また、書き込み可能なDVD装置もしくはデジタル方式のVTRであれば必要なフォーマット変換の後書き込み保存される。

#### 【0032】

もし履歴情報の中に相手側の機器IDが含まれていない場合、コマンド入力手段10に対してユーザからAVデータ送信指示が来るのを待つ。コマンド入力、すなわちAVデータ送信指示があると、認証手段50は相手側の認証手段140と認証を行う。認証を終えると、認証履歴記憶手段80に相手側の機器IDを履歴情報として記録する。AVデータ送信手段30はAVデータの送信を開始する。AVデータは暗号化手段40において暗号鍵を用いて暗号化され入出力手段60を介して伝送路に送出される。相手側の送受信機器において、入出力手段110は伝送路から暗号化されたAVデータを受け取る。復号化手段130は暗号化されたAVデータを暗号鍵を用いて復号し、AVデータ受信手段120は復号化されたAVデータを受け取る。

#### 【0033】

図2は本発明の第1の実施の形態の著作物保護システムの動作状態を示す遷移図である。図2を参照すると、機器ID検出手段70は相手側の機器IDを検出する(S1)。次に、認証履歴記憶手段80が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる(S2)。もし、履歴情報の中にその機器IDが含まれている場合、認証手段50は相手側の認証手段140と認証を行う(S3)。その後、コマンド入力手段10に対してユーザからAVデータ送信指示があると(S4)、コマンド制御手段20を介してAVデータ送信手段30にそのコマンドが通知され、AVデータ送信手段30はAVデータの送信を開始する(S5)。

#### 【0034】

もし履歴情報の中に機器IDが含まれていない場合、コマンド入力手段10に対してユーザからAVデータ送信指示が来るのを待つ。AVデータ送信指示があると(S6)、認証手段50は相手側の認証手段140と認証を行う(S7)。認証を終えると、認証履歴記憶手段80に相手側の機器IDを履歴情報として記

録する（S8）。AVデータ送信手段30はAVデータの送信を開始する（S5）。

## 【0035】

その後の繰り返し動作においては、認証履歴のその機器IDが記録されているため、認証手段50が認証を行い（S3）、コマンド入力手段10に対してユーザからAVデータ送信指示があると（S4）、コマンド制御手段20を介してAVデータ送信手段30にそのコマンドが通知され、AVデータ送信手段30はAVデータの送信を開始する（S5）。

## 【0036】

（本発明の第2の実施の形態）

次に、本発明の第2の実施の形態について図面を参照して詳細に説明する。

## 【0037】

図3を参照すると本実施の形態は著作物伝送する相手側の送受信機器を複数備えて構成される。すなわち、機器ID検出手段70は送受信機器が伝送路に接続すると、入出力手段60を介して、その機器IDを検出する。機器ID検出手段70が第一の相手側の送受信機器の機器IDを検出すると、認証履歴記憶手段80が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる。もし、履歴情報の中にその機器IDが含まれている場合、認証手段50は相手側の認証手段140と認証を行い、鍵共有の結果、暗号鍵を得る。その暗号鍵を第一の暗号鍵として暗号鍵記憶手段90に記録する。また、機器ID検出手段70が第二の相手側の送受信機器の機器IDを検出すると、認証履歴記憶手段80が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる。もし、履歴情報の中にその機器IDが含まれている場合、認証手段50は相手側の認証手段240と認証を行い、鍵共有の結果、暗号鍵を得る。その暗号鍵を第二の暗号鍵として暗号鍵記憶手段90に記録する。

## 【0038】

履歴情報の中に第一の相手側の送受信機器IDが含まれていない場合は、コマンド入力手段10に対してユーザから第一の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があるのを待つ。そのAVデータ送信指示のコマ

ンド入力があると、認証手段50により、第一の相手側の認証手段140と機器認証作業と鍵交換作業とを行う。機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段80に第一の相手側の送受信機器IDを履歴情報として記録する。鍵交換作業の結果、共有した暗号鍵を第一の暗号鍵として暗号鍵記憶手段90に記録する。

## 【0039】

履歴情報の中に第二の相手側の送受信機器IDが含まれていない場合、コマンド入力手段10に対してユーザから第二の相手側の送受信機器に対してのAVデータ送信指示のコマンド入力があるのを待つ。そのAVデータ送信指示のコマンド入力があると、認証手段50により、第二の相手側の認証手段240と機器認証作業と鍵交換作業とを行う。機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段80に第二の相手側の送受信機器IDを履歴情報として記録する。鍵交換作業の結果、共有した暗号鍵を第二の暗号鍵として暗号鍵記憶手段90に記録する。

## 【0040】

認証および暗号鍵の記録を終えると、その後いつでも、コマンド入力手段10に対してユーザから第一の相手側の送受信機器に対してのAVデータ送信指示があると、コマンド制御手段20を介してAVデータ送信手段30にそのコマンドが通知され、AVデータ送信手段30はAVデータの送信を開始する。AVデータは暗号鍵記憶手段90に記録されている第一の相手側の送受信機器用の暗号鍵を用いて暗号化手段40において暗号化され入出力手段60を介して伝送路に送出される。第一の相手側の送受信機器において、入出力手段110は伝送路から暗号化されたAVデータを受け取る。復号化手段130は暗号化されたAVデータを第一の相手側の送受信機器用の暗号鍵を用いて復号し、AVデータ受信手段120は復号化されたAVデータを受け取る。

## 【0041】

また、コマンド入力手段10に対してユーザから第二の相手側の送受信機器に対してのAVデータ送信指示があると、コマンド制御手段20を介してAVデータ送信手段30にそのコマンドが通知され、AVデータ送信手段30はAVデー

タの送信を開始する。A Vデータは暗号鍵記憶手段90に記録されている第二の相手側の送受信機器用の暗号鍵を用いて暗号化手段40において暗号化され入出力手段60を介して伝送路に送出される。第二の相手側の送受信機器において、入出力手段210は伝送路から暗号化されたA Vデータを受け取る。復号化手段230は暗号化されたA Vデータを第二の相手側の送受信機器用の暗号鍵を用いて復号し、A Vデータ受信手段220は復号化されたA Vデータを受け取る。

## 【0042】

本実施の形態で明らかなように本発明の著作物保護方式および装置は相手側の送受信機器が複数存在する場合においても、ユーザから著作物伝送を指示するコマンドを入力した時点から著作物伝送開始までの時間を従来に比較して大幅に短縮できる効果を有する。

## 【0043】

また、ここまでの説明においては、コマンド入力手段10ならびにコマンド制御手段20がA Vデータ送信機器に具備されて構成する例を示したが、コマンド入力手段10ならびにコマンド制御手段20はA Vデータ送信機器に具備されないで構成することも可能である。

## 【0044】

さらに、ここまでの説明においてはA Vデータ送信機器が一つで構成する例について述べたが、本発明による効果を何ら失うことなしに、複数のA Vデータ送信機器が存在する構成とすることも勿論可能である。

## 【0045】

そして、図1および図3の実施の形態において認証履歴記憶手段80を含まない構成とする実施の形態も本発明の別の実施の形態である。この実施の形態においては、送受信機器が伝送路に接続され、機器ID検出手段70がその機器IDを検出すると、履歴情報とは無関係に、認証手段50は相手側の認証手段と認証を行う。本実施の形態においては、履歴情報とは無関係に認証を行うので、新たなA Vデータ送信機器が接続して最初の著作物伝送においても、時間を従来に比較して大幅に短縮できる効果を持つことが明らかである。

## 【0046】

【発明の効果】

以上説明したように、本発明は、ユーザから著作物伝送を指示するコマンドを入力した時点から著作物伝送開始までの時間を従来に比較して大幅に短縮できるという効果がある。

【0047】

その理由は過去に認証を行った履歴がある送受信機器が伝送路に接続すると、ユーザからのコマンド入力が行われる以前に機器認証および鍵交換を行うためである。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態の著作物保護システムの構成を示すブロック図である。

【図2】

本発明の第1の実施の形態の著作物保護システムの動作状態を示す遷移図である。

【図3】

本発明の第2の実施の形態の著作物保護システムの構成を示すブロック図である。

【図4】

従来の著作物保護システムのブロック図である。

【図5】

従来の著作物保護システムの状態遷移図である。

【符号の説明】

- |                   |           |
|-------------------|-----------|
| 10、11             | コマンド入力手段  |
| 20、21             | コマンド制御手段  |
| 30、31             | AVデータ送信手段 |
| 40、41             | 暗号化手段     |
| 50、51、140、141、240 | 認証手段      |
| 60、61、110、111、210 | 入出力手段     |



70 機器ID検出手段

80 認証履歴記憶手段

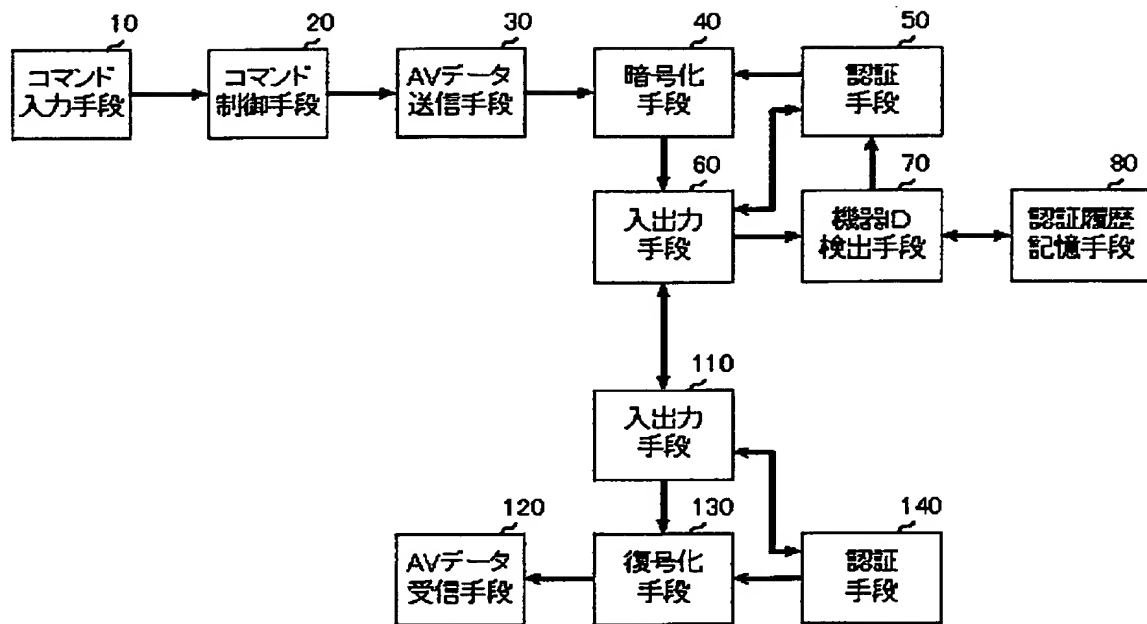
90 暗号鍵記憶手段

120、121、220 AVデータ受信手段

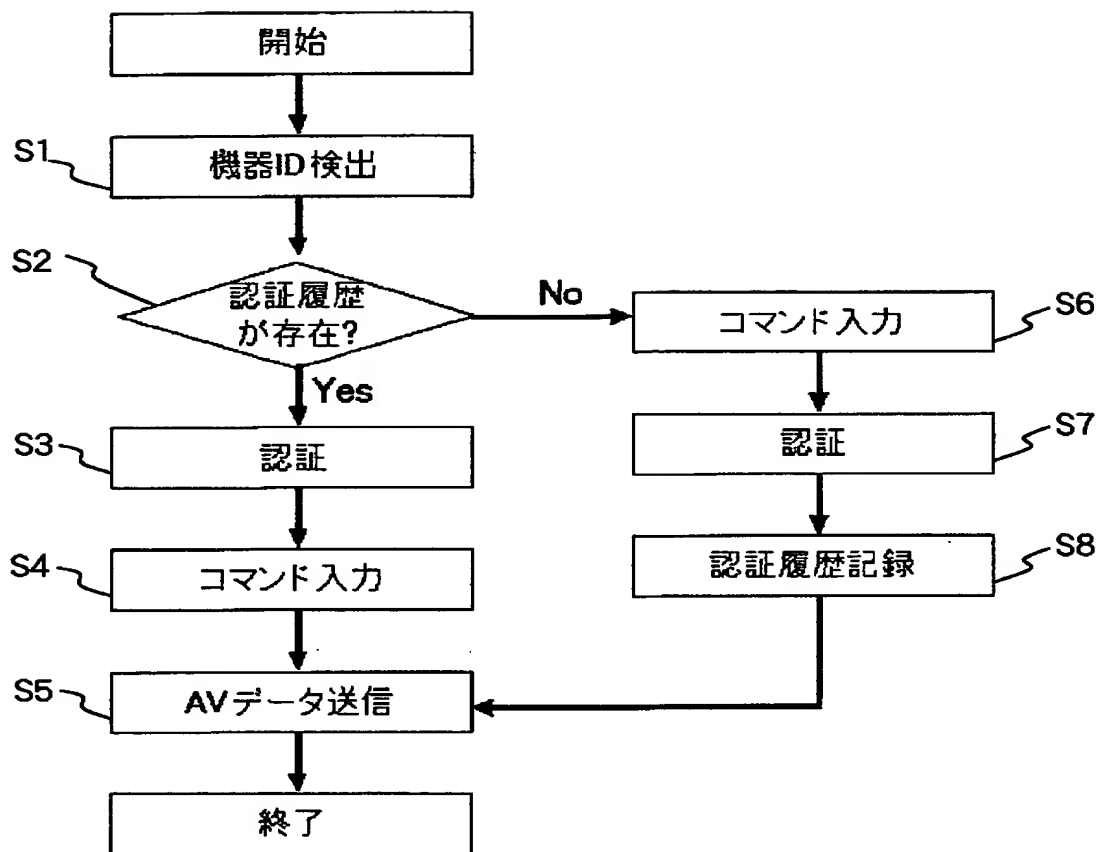
130、131、230 複号化手段

【書類名】 図面

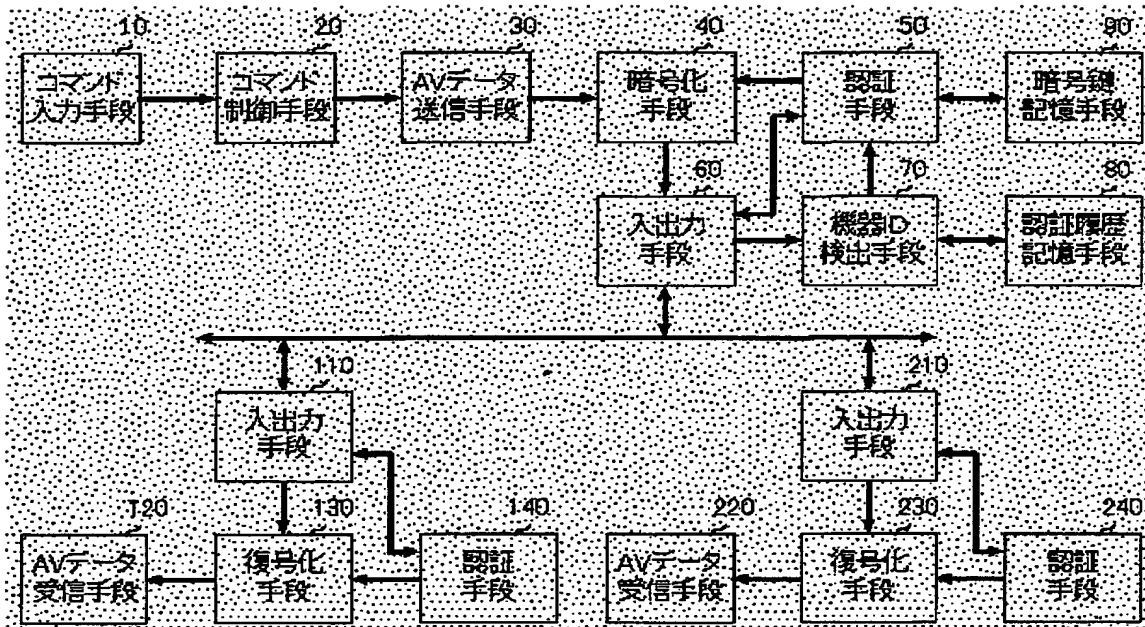
【図 1】



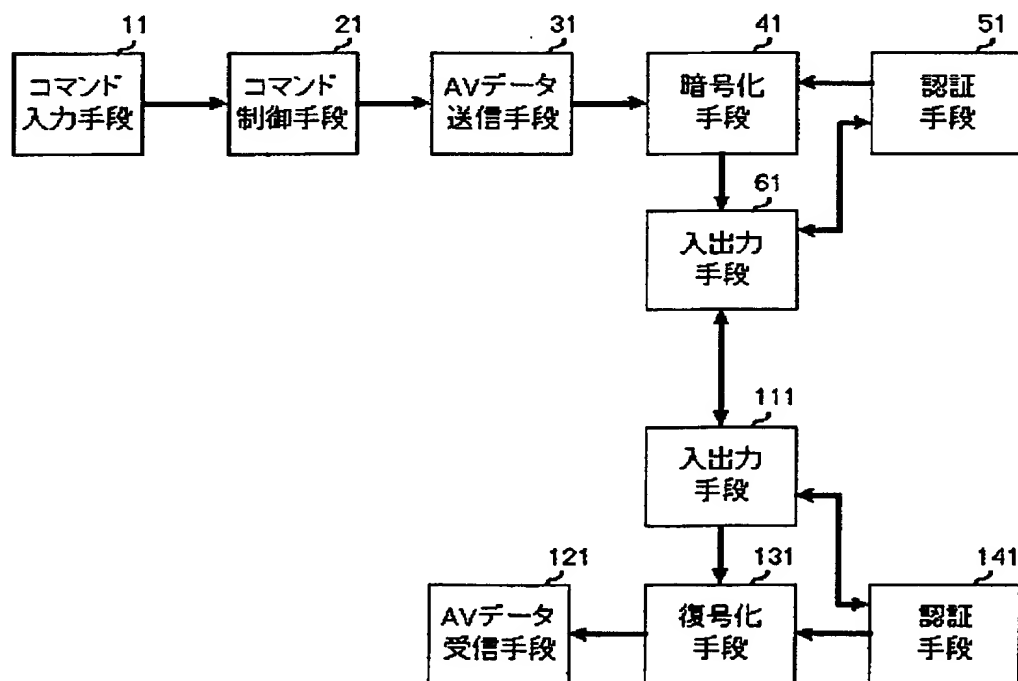
【図 2】



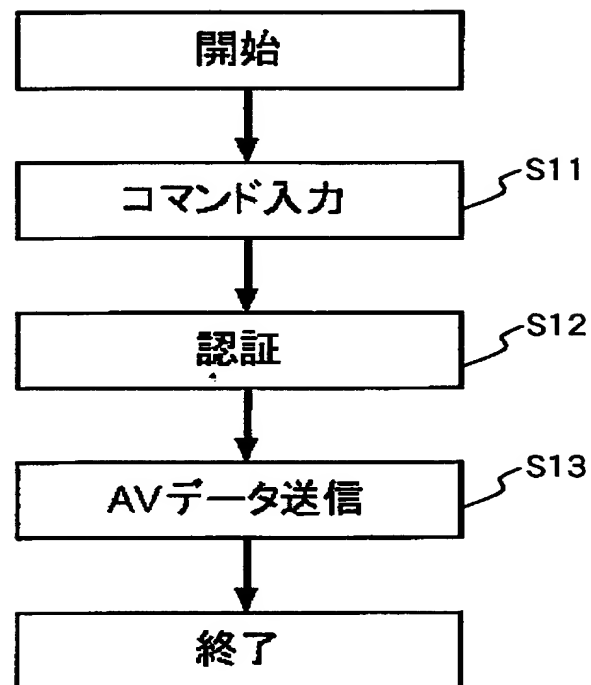
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 AVデータ伝送指示からAVデータを伝送するまでの時間を短縮する著作物保護システム及びその著作物保護方法を提供することにある。

【解決手段】 機器ID検出手段70は相手側の機器IDを検出する。次に、認証履歴記憶手段80が記憶している履歴情報の中にその機器IDが含まれているかどうかを調べる。もし、履歴情報の中にその機器IDが含まれている場合、認証手段50は相手側の認証手段140と認証を行う。その後、コマンド入力手段10に対してユーザからAVデータ送信指示があると、コマンド制御手段20を介してAVデータ送信手段30にそのコマンドが通知され、AVデータ送信手段30はAVデータの送信を開始する。

【選択図】 図1

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000004237  
【住所又は居所】 東京都港区芝五丁目7番1号  
【氏名又は名称】 日本電気株式会社

【代理人】 申請人

【識別番号】 100070219  
【住所又は居所】 東京都港区赤坂1丁目9番20号 第16興和ビル  
8階 若林国際特許事務所  
【氏名又は名称】 若林 忠

【選任した代理人】

【識別番号】 100100893  
【住所又は居所】 東京都港区赤坂1丁目9番20号 第16興和ビル  
8階  
【氏名又は名称】 渡辺 勝

【選任した代理人】

【識別番号】 100088328  
【住所又は居所】 東京都港区赤坂1丁目9番20号 第16興和ビル  
8階  
【氏名又は名称】 金田 暢之

【選任した代理人】

【識別番号】 100106138  
【住所又は居所】 東京都港区赤坂1丁目9番20号 第16興和ビル  
8階  
【氏名又は名称】 石橋 政幸

【選任した代理人】

【識別番号】 100106297  
【住所又は居所】 東京都港区赤坂1丁目9番20号 第16興和ビル  
8階 若林国際特許事務所  
【氏名又は名称】 伊藤 克博

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社